Cyber Security Officer

Department: Directorate of Technology Estates and Facilities

Hours of work: Full time | 37 hours per week

Contract type: Open

Salary: Grade 6 | £34,308 - £42,155 per year
Introduction

The Directorate of Technology, Estates and Facilities (DTEF) is responsible for ‘providing outstanding work, study, research facilities, and facilities to enhance the student experience, on campus and online’.

The role will be part of the cyber security team within IT Services.

Main Purpose of the role

Cyber Security is a key priority at the University of York. Through investment from the University Executive Board the Cyber Security Team must maintain an updated position in order to continue to meet the ever changing landscape of Information Security.

The Cyber Security Officer will report to the Head of Cyber Security and will lead security engagement across ITS and other technical teams within the University. Interpretation of security standards and university policy then providing requirements, functional guidances and security testing assurances.

Key responsibilities

(Role holders will be required to undertake some or all of the duties below)

1. Role Specific Responsibilities

   Cyber Security
   - Identify the need for new and enhanced IT security systems, developing the Universities requirements for new tooling and leading supplier engagement.
   - As part of the Cyber Security Team you will ensure the security process is documented, maintained, deployed in line with requirements of our specifications and will achieve compliance with selected standards.

   Security Service
   - Managing tasks to proactively deliver an Information security advice and assurance service to internal contacts.
   - Defining service level agreements for the service and market to Academic and Professional Support staff.

   Strategy
   - As required you will contribute to or lead the development of requirements, liaison with specific suppliers or the implementation of new services, this includes liaising with and gathering requirements from across ITS.

   Security by Design
   - Participate in departmental (ITS) and external projects or teams requiring expertise in cyber security, ensuring security requirements and Security by Design principles are implemented and followed as required.

   Incident Management
   - In conjunction with the Head of Cyber Security, manage cyber security incidents and direct investigations where issues and incidents have occurred. Providing oversight for the identification,
triage and response to events or incidents that may indicate a security breach, ensuring that colleagues within, with Cyber Security and ITS are engaged for incident response.

- You will directly liaise with university departments and faculties on incidents and track recommendations and improvements resulting from post incident assessments.

**Security Testing**

- Maintain the relationships with external partners; penetration testers, accreditors, Managed SOC providers etc. to ensure that the delivered service is meeting the expectations of the University of York and this is validated within the Cyber Security functions, across ITS and other dependent areas of the university.
- Review vulnerability management reports and penetration test reports and liaise with other Cyber Security and IT Services colleagues to identify and implement fixes to address these vulnerabilities, maintaining a record of identified issues and remediation actions.

**Standards & Compliance**

- Ensure that the University's statements and assurances around security related accreditations and assessments; ISO27001, Cyber Essentials, PCI DSS, are correct and escalate where you identify issues or risks, through liaison with faculties and departments owning or dependant on certifications.
- Conduct reviews and assessments of selected standards to ensure that compliance can be demonstrated to internal and external audit or assessment.

2. **University of York Responsibilities for Grade 6**

**Service and Operational Delivery**

- Oversee a responsive and proactive support service to ensure service expectations are met.
- Collect and analyse stakeholder feedback to help define needs and requirements and the design and planning of services.
- Contribute to operational leadership teams and decision making to shape the nature and level of support services.
- Implement changes to the design and development of a service.
- Accountable for delivery of a service within a defined area or defined responsibilities.
- Make effective use of digital solutions to carry out operational activity and implement efficiency improvements.
- Depending on the role, may be required to act as operational line manager - setting, monitoring and overseeing the work of the team on a day to day basis.

**Continuous Improvement**

- Analyse service and operational delivery data and provide reports, making recommendations for improvement as appropriate.
- Ensure the review and improvement of systems and procedures in line with University frameworks.
- Review internal and external practice to identify opportunities for future improvements or efficiencies.
- Apply expertise to identify, understand and propose resolutions for issues or problems.
● Proactively identify opportunities for building personal knowledge and skills, and ensure training and development needs of the team are met.
● Deliver knowledge sharing on specialist defined processes across the broader team.

Specialist Contribution
● Provide advice to stakeholders in relation to complex policy, procedures and regulations.
● Provide specific technical advice to ensure compliance with legislation, statutory duties, etc.
● Provide specialist expertise and support with complexity of data and information sources, providing interpretation and analysis.
● Carry out in-depth, complex investigations or searches; interrogate the information and data to identify trends and patterns.
● Deliver training, teaching and/or development delivery for stakeholders.

Collaboration and Communication
● Establish, maintain and develop productive and ongoing relationships with University stakeholders to create ideas for tactical service or operational delivery development.
● Build relationships and networks internally and externally to build and update knowledge and skills.
● Use a range of digital media and tools to communicate with a diverse range of key stakeholders.
● Act as a supportive and encouraging member of a team. For roles at this level with supervisory responsibilities, demonstrate compassion and give advice on commonly occurring wellbeing issues.

Governance and Oversight
● Oversee activity to ensure all processes and transactions are delivered in line with regulatory and professional service and policy standards.
● Provide advice and training to stakeholders regarding compliance and regulations relating to the area of responsibility.
● Contribute to the creation or development of policy and procedures to take account of internal and external changes.
● Ensure activities and documents comply with internal University and external regulation, policy and procedures.

Planning and Organisation
● Plan, organise and prioritise the work of self and team members on a regular basis, taking into account operational needs and changing circumstances over the short to mid term.
● Contribute to longer term strategic /planning of the team’s work.
● Lead the delivery of projects to facilitate service operational change or play a role in University-wide projects.

The above list of duties is not exhaustive and is subject to change. The post holder may be required to undertake others duties within the scope and grading of the post.
## Person specification

<table>
<thead>
<tr>
<th>Role Specific</th>
<th>Essential / Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experience in assessing security requirements and ensuring their implementation and delivery can be measured and evidenced.</td>
<td>Essential</td>
</tr>
<tr>
<td>Experience in assessing risk and communicating security technical documentation in a manner that non-IT colleagues will understand.</td>
<td>Essential</td>
</tr>
<tr>
<td>Ability to collaborate with colleagues within and outside ITS and subject matter experts around the university to align and support differing agendas.</td>
<td>Essential</td>
</tr>
<tr>
<td>Familiarity with information security standards (ISO, CE, PCI, CIS, NIST) and demonstrable capabilities in 4 security domains areas of the CIS V8 control areas.</td>
<td>Essential</td>
</tr>
<tr>
<td>Management of key suppliers in delivery of service, support and consultancy to ensure value and benefit is being received and can be evidenced in improvement.</td>
<td>Desirable</td>
</tr>
<tr>
<td>Experience in leading security testing services; test specifications, test completion and remediation of identified issues.</td>
<td>Desirable</td>
</tr>
</tbody>
</table>

**University of York Person Specification for Grade 6**

**Qualifications:**

Level 3 qualification. (Qualifications at this level include A levels. Please see the full list). We also welcome applicants with equivalent non-UK qualifications or equivalent professional experience. **Essential**

**Skills - demonstrates the ability to:**

- Lead projects **Essential**
- Gather, analyse, interpret and report complex data/information **Essential**
- Use digital technologies including Google applications and/or Microsoft Office **Essential**
- Communicate effectively in verbal and written formats, including the use of a variety of digital tools **Essential**

**Behaviours:**

- Works collaboratively with others **Essential**
- Delivers a quality service **Essential**
- Develops self and others **Essential**
<table>
<thead>
<tr>
<th>Actively champions respect, inclusivity, equality and diversity</th>
<th>Essential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies and implements continuous improvement</td>
<td>Essential</td>
</tr>
</tbody>
</table>